View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by University of Strathclyde Institutional Repository

Learning from accidents: investigating the genesis of human errors in multi-attribute settings to improve the organisation of design

R. Moura[a,d] , M. Beer[b,a,c], E. Patelli[a] & J. Lewis[a]
[a]*Institute for Risk and Uncertainty, University of Liverpool, United Kingdom*
[b]*Institute for Computer Science in Civil Engineering, Leibniz University Hannover, Germany*
[c]*Tongji University, Shanghai, China*
[d]*National Agency for Petroleum, Natural Gas and Biofuels (ANP), Brazil*

F. Knoll
NCK Inc., Montreal, Canada

ABSTRACT: Latest disasters in high-technology systems, such as the February 2016 train collision in southern Bavaria, Germany (BBC,2016), have been associated with complex interactions between design shortcomings, human factors and organisations. In an attempt to approach this important matter and improve the interfaces between humans, technology and organisations, this paper first applies an unsupervised learning neural network approach entitled self-organising maps (SOM) to a dataset containing 238 major accidents collected from industry, regulators and insurance companies. The data mining process translated extremely complex data into a 2-D topographical map, ordered by similarity. Results highlighted a portion of the map where the worst consequences of the accidents were observed, using the fatalities rate as a metric. Relevant relationships between design failures and human factors were exposed, and several examples extracted from the targeted cluster had been presented. The findings emerging from the lessons learned from major accidents were then translated into a practical guide for designers and design reviewers, also revealing opportunities to expand designers' understanding and perception of risks related to human factors.

1 INTRODUCTION

Remarkable advances in engineering and system controls in recent times and the consequent development of state-of-the-art technologies are clearly resulting in economic, environmental and safety benefits to the society. Latest disasters, however, put human error in the glare of the media spotlight. The February 2016 train collision in southern Bavaria, Germany, which took 11 lives and left more than 90 people injured, is one of several examples where human errors appear to have played a significant role in a major accident. Despite the fact that investigations are still ongoing and a final report has not been issued, the chief prosecutor anticipated that a local controller opened the track to two trains simultaneously, and his erroneous actions had catastrophic consequences (BBC, 2016). The railway system has multiple safety barriers in place, such as an automatic braking system if a train crosses a stop signal, but the track controller had reportedly disabled it. When he recognised the error and tried to warn the drivers, it was too late.

It is clear that the designed safety features were not sufficient to minimise the possibility of human error, even if investigators rule out technical problems and equipment failures. A head-on collision involving two trains is obviously a critical scenario, which should have been avoided by multiple safety barriers (track control, signalling system, automatic stoppage etc). If a single track controller is capable of interfering with the technology by overriding all barriers at once, there might be serious issues with the conception of the system: i.e. safety barriers should be independent, and if they can be simultaneously deactivated, they should have been considered as a single barrier, in a general design perspective.

Moreover, previous work involving the statistical analysis of major accidents (Moura et al, 2016) has shown that around 73% of the erroneous actions identified during in-depth investigations were combined with some kind of design shortcoming to generate a catastrophic outcome. The link between human errors and design failures became apparent, as well as the indication that an effective design management strategy that considers human behaviour could be crucial to reduce the chances of having a major accident such as the rail accident previously described.

The idea of human-centred design (Boy, 2013; Kurosu, 2011) placed the human being as a critical component in the design considerations, taking into account the psychological and physiological characteristics, along with the technology and the operational environment. In an objective way, it is not the operators that will need to adapt to the systems, but

systems will have to be suited to the users' needs. However, the scarcity of human performance data in complex systems is a well-known limitation (Moura et al., 2015a; Swain, 1990) to the development of an effective design strategy. Collecting data and generating means to prevent major accidents is a challenging effort, especially if systemic events are prioritised over the more trivial ergonomic and occupational accidents such as slips, trips and falls.

Therefore, further investigation into the interactions between humans, technologies and organisations through the detailed analysis of historical data may disclose reasonable clues on the genesis of human errors.

Previous research comprised data generated from occupational to serious accidents (Bellamy, 2007, 2013) or limited the domain to a single industry (Baysari et al, 2008; Evans, 2011). Conversely, the current research encompassed major accidents from different industries (e.g. oil & gas upstream, refineries, aviation, nuclear and transportation). All events were thoroughly scrutinised by investigation teams in the search for causes, and the information provided is very detailed and reliable. The aim is to expose the intricate conditions leading to these rare events, giving some indications on how to tackle human factors issues by improving design, in terms of suitability and prevention of erroneous actions.

2 BACKGROUND

Moura et al. (2016) have translated a collection of 238 major accident reports from different industrial backgrounds into a common framework, in order to make the data comparable. The reports were obtained from regulators, internal investigations conducted by industry, independent investigation commissions and insurance companies, containing very detailed descriptions of the triggering events and contributing factors to the events. The complete list of reporting entities and further details on the construction of the dataset can be found in Moura et al. (2015a).

Different contributing factors derived from Hollnagel's (1998) Contextual Control Model used as basis for the Cognitive Reliability and Error Analysis Mode (CREAM) were identified and tabulated, resulting in the construction of the Multi-attribute Technological Accidents Dataset (MATA-D).

The dataset contains a Boolean representation (i.e. presence or absence) of 53 contributing factors in the lower level of the hierarchy, which are distributed between 15 different classes. These are all linked to 3 major categories: Man, Technology and Organisation. Having the factors identified for each one of the accidents, statistical analyses as well as the application of data mining approaches were made possible.

Previous research applied different methods to disclose relevant associations within the MATA-D dataset.

Moura et al (2015b) successfully used in earlier versions of the dataset an unsupervised artificial neural networks approach. As a result, a relationship between design failures and the lack of training was initially found, which influenced erroneous interpretations and action failures. In addition, a general configuration for human errors in industrial accidents was developed, disclosing some organisational factors disturbing human cognitive functions.

Moreover, Doell et al (2015) also tested association rule mining techniques on both the lower (53 factors) and the intermediate (15 factors) hierarchical levels of the MATA-D dataset, aiming at the identification of relevant links among contributing factors. Attributes that occurred infrequently had to be excluded from the analysis, due to limitations in the extraction of association rules, but these were assessed separately. Links between action failures and specific cognitive functions; wrong reasoning and inadequate task allocation; and design failures and insufficient knowledge were identified.

A tailored Hierarchical Agglomerative Clustering method (Moura et al, 2015c) was also applied to 202 of the 216 events that were in the dataset at the time of the analysis. It was necessary to leave single-cause accidents out of the analysis, as these would appear as outliers. In that work, the clustering focused on the intermediate level of the MATA-D dataset hierarchy (action error, specific cognitive functions, temporary person related functions, permanent person related functions, equipment, procedures, temporary interface, permanent interface, communication, organisation, training, ambient conditions and working conditions) and a relationship between specific cognitive functions and the deadliest group of accidents was suggested.

Previous work using MATA-D (Doell et al., 2015; Moura et al.,2015b, 2015c) concentrated on finding the most relevant factors and disclosing key relationships among them, by applying a number of data mining approaches to the Boolean data contained in earlier versions of the proprietary dataset. Now, the objective is to go beyond the binary information appraisal, using a clustering approach as a pre-processing technique, and then revealing specific features in the design lifecycle, which might have led to the most serious consequences to human life.

3 ANALYSIS METHOD

The MATA-D dataset version presented by Moura et al. (2016), which contains 238 major accidents, was subjected to an unsupervised learning neural network approach entitled self-organising maps (SOM) (Kohonen, 2001). SOM has been used in many dif-

ferent data mining applications, where visualisation of high-dimensional data is required (Kohonen, 2013; Ultsch, 1993). The intention was to have the data reorganised in the output space by accidents' similarity, using as input data the 53 possible contributing factors for each single event, i.e. a matrix 238 x 53.

Basically, the method (Kohonen, 2001) involves the training of the neural network according to

$$v(t) = \arg\min_{i \in \Omega} \|x(t) - m_i(t)\| \quad (1)$$

where $v(t)$ = the minimum distance between the input vector $x(t)$ and a node m_i in the output space.

Then, the convergence of the output space is obtained through the batch-learning version of the algorithm (Eq. 2), as recommended by Kohonen (2013) for practical applications.

$$m_i^* = \frac{\sum_j n_j h_{ji} \overline{x_j}}{\sum_j n_j h_{ji}} \quad (2)$$

where m_i^* = best matching node; $\overline{x_j}$ = x(t) mean value; n_j = number of samples; and h_{ji} = neighbourhood of the m_i.

The output provided by the application of the Kohonen algorithm described above results in a 2-D array, ordered in a topographic arrangement where similar accidents (considering the occurrence of the contributing factors) are aggregated in one of the four clusters (Fig. 1). The expert version of the Viscovery® SOMine software was used to generate graphs.

Having the accidents ordered by similarity, the statistical analysis of the resulting clusters (presented in Table 1) revealed important features, which were used as criteria to define the group(s) of interest. Therefore, portions of the map where the worst consequences of the accidents were observed could be highlighted for further consideration, using the fatalities rate as a metric.

Once the cluster of interest has been defined, relevant relationships between design failures, human factors and technology were exposed, presenting the factors which contributed to the accidents with the most disastrous consequences. Further data from the MATA-D dataset were then retrieved, bringing into light the detailed descriptions of the design failures for the evaluated cluster, and the interaction of these shortcomings with other relevant aspects had been explained.

The data mining effort continued by the identification of the design lifecycle stage where the failures were most likely produced, also identifying the disciplines which improvements would generate a benefit in terms of safety, by assisting the prevention of human errors.

The findings served as a basis for the development of a general framework, intended to provide designers and reviewers with some guidance on how to identify and tackle possible gaps and shortcomings during the design stage.

4 RESULTS

Figure 1 represents the clustering results of the MATA-D dataset, using the self-organising maps. Table 1 shows the number of accidents, the fatalities rate and the frequency of all identified factors per cluster, presenting all characteristics of the resulting groupings.

Accidents involving design failures were mostly grouped in Cluster 3, where design issues appeared in 87.2% of the featured accidents, and in Cluster 1, where 85% of the accidents presented a design fault as a contributing factor. Quality control problems were also highlighted in both clusters 1 and 3, with 81.3% and 79.5%, respectively. Furthermore, training aspects (insufficient skills, with 56.3% and 76.9%, and insufficient knowledge, with 60% and 56.4%) were significant in the two clusters.

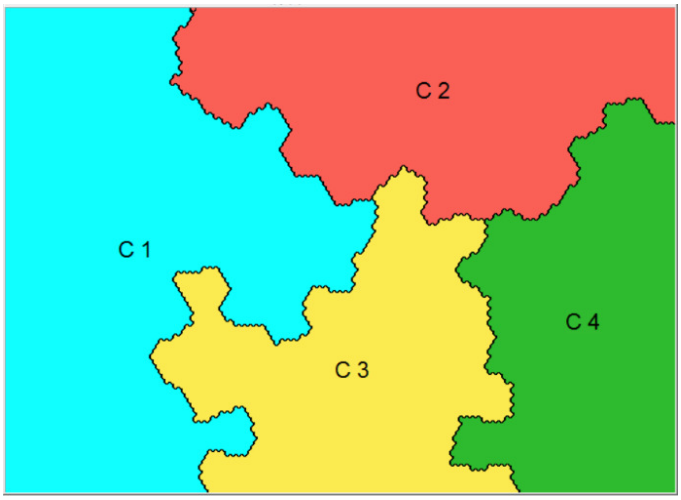

Figure 1. MATA-D Clustering Results using SOM

Nonetheless, major accidents are considered to be rare events, resulting from a complex interaction of numerous aspects (Reason, 1997). Therefore, in spite of having some similarities, the genesis of the major accidents affected by design failures, largely represented by Clusters 1 and 3, lies in dissimilar groups of human, technological and organisational factors.

Action errors in Cluster 1 were largely identified as a failure to perform a sequence of actions (wrong place), appearing in 52.5% of the cluster accidents. Conversely, human errors identified in Cluster 3 were mainly wrong time (41%) and wrong type (30.8%). Accidents in Cluster 3 also posed more complex challenges to the human cognitive functions, as a significant failure in the operators' mental plan was identified in many cases – 25.6% of inadequate plan and 15.4% of priority error.

From a technological perspective, Cluster 1 accidents were influenced by inadequate procedures (78.7%) and incomplete information from the inter-

face (36.2%), while Cluster 3 accidents were severely affected by equipment failures, with 94.9% of incidence.

There is also a significant contrast between organisational aspects within these two clusters. Cluster 1 noteworthy genotypes included a very significant contribution of the inadequate task allocation factor, with 95% of incidence, along with maintenance failure (56.3%) and missing information (37.5%). Instead, factors in Cluster 3 that were significantly above the overall incidence average were management problem (23.1%) and communication failure (20.5%).

The 53 factors extracted from the CREAM framework are listed and divided by Human Factors (erroneous actions, observation, interpretation, planning, temporary person-related functions and permanent person-related functions); Technology (equipment failure, procedures, temporary interface problems and permanent interface problems) and Organisation (organisational issues, training, ambient conditions and working conditions).

Table 1. Clustering Results

Cluster Id.	Cluster 1	Cluster 2	Cluster 3	Cluster 4
Accidents #	80	57	39	62
Fatalities Rate	4.65	1.68	19.71	4.63
Wrong Time	13.8%	10.5%	41.0%	3.2%
Wrong Type	11.3%	7.0%	30.8%	4.8%
Wrong Object	3.7%	3.5%	2.6%	0.0%
Wrong Place	52.5%	36.8%	12.8%	11.3%
Observation Missed	20.0%	12.3%	23.1%	8.1%
False Observation	6.3%	3.5%	0.0%	1.6%
Wrong Identification	5.0%	0.0%	5.1%	0.0%
Faulty Diagnosis	26.3%	8.8%	12.8%	0.0%
Wrong Reasoning	20.0%	1.8%	25.6%	0.0%
Decision error	5.0%	17.5%	17.9%	1.6%
Interpretation delay	8.7%	1.8%	7.7%	0.0%
Incorrect Prediction	7.5%	1.8%	2.6%	1.6%
Inadequate Plan	10.0%	7.0%	25.6%	1.6%
Priority error	6.3%	8.8%	15.4%	1.6%
Memory failure	1.3%	1.8%	0.0%	0.0%
Fear	1.3%	0.0%	5.1%	3.2%
Distraction	11.3%	3.5%	7.7%	0.0%
Fatigue	7.5%	0.0%	2.6%	0.0%
Perform. Variability	5.0%	1.8%	0.0%	0.0%
Inattention	2.5%	0.0%	5.1%	1.6%
Physiological Stress	1.3%	1.8%	0.0%	0.0%
Psychological Stress	5.0%	1.8%	2.6%	1.6%
Functional Impairm.	0.0%	0.0%	2.6%	0.0%
Cognitive Style	0.0%	0.0%	0.0%	0.0%
Cognitive Bias	15.0%	1.8%	10.3%	0.0%
Equipment Failure	33.8%	22.8%	94.9%	87.1%
Software Fault	6.3%	0.0%	2.6%	0.0%
Inadeq. Procedure	78.7%	42.1%	38.5%	4.8%
Access Limitations	3.7%	0.0%	0.0%	0.0%
Ambiguous Info.	5.0%	0.0%	5.1%	0.0%
Incomplete Info.	36.2%	7.0%	20.5%	1.6%
Access Problems	3.7%	0.0%	2.6%	0.0%
Mislabelling	2.5%	1.8%	0.0%	1.6%
Communic. Failure	16.3%	5.3%	20.5%	1.6%
Missing Information	37.5%	14.0%	15.4%	8.1%
Maintenance Failure	56.3%	14.0%	33.3%	27.4%
Inad. Quality Control	81.3%	24.6%	79.5%	56.5%
Management Prob.	12.5%	5.3%	23.1%	0.0%
Design Failure	85.0%	50.9%	87.2%	41.9%
Task Allocation	95.0%	68.4%	48.7%	14.5%
Social Pressure	17.5%	3.5%	0.0%	1.6%
Insufficient Skills	56.3%	12.3%	76.9%	6.5%
Insuffic. Knowledge	60.0%	17.5%	56.4%	6.5%
Temperature	1.3%	0.0%	2.6%	1.6%
Sound	0.0%	0.0%	0.0%	0.0%
Humidity	0.0%	0.0%	0.0%	0.0%
Illumination	1.3%	1.8%	0.0%	0.0%
Other	0.0%	0.0%	0.0%	0.0%
Ambient Conditions	2.5%	14.0%	10.3%	4.8%
Excessive Demand	6.3%	8.8%	5.1%	1.6%
Work Place Layout	1.3%	7.0%	2.6%	0.0%
Inad. Team Support	6.3%	0.0%	7.7%	0.0%
Irreg. Working hours	10.0%	1.8%	0.0%	0.0%

However, what makes Cluster 3 remarkably different from the remaining groupings is the impact of the accidents in terms of fatalities. While Clusters 1, 2 and 4 presented a fatality rate, respectively, of 4.65, 1.68 and 4.63 deaths per major accident, Cluster 3 had a record of 19.71 fatalities per event. It is important to notice that fatalities figures were not applied to the SOM algorithm as input data to group accidents by any means, implying that the correspondence among these events is exclusively due to the contributing factors.

The results from Cluster 3, which contained the most lethal group of events, also suggest a strong link between design failures and human errors: all accidents involving fatalities in Cluster 3 had a design fault, and some sort of human error was observed in 81.25% of these cases. As the SOM clustering considered the whole range of specific factors (53 in total), it is now possible to relate design failures with specific human errors, disclosing precise erroneous action types and cognitive functions.

Regarding the analysis of the interfaces between design and human factors in Cluster 3 accidents, 53.84% of the design faults affected complex cognitive functions, influencing the formulation of mental plans to understand an unexpected situation. 30.77% of the design failures were linked to the human's capacity to interpret signals and act properly. Finally, the remaining 15.38% of design shortcomings were associated with the failure to observe a signal and recover from the accidental path.

Simple and fundamental design faults, mostly related to materials selection or layout, appeared in all remaining major events. Examples are the usage of a polyvinylchloride pipe to transport inflammable liquids aboveground, instead of steel, or placing hydro-

carbon tanks within the legs of a floating platform, severely compromising the maritime unit's buoyancy in case of a tank failure.

Table 2 lists many cases of design failures linked to major accidents with multiple fatalities as grouped in Cluster 3, giving detailed information about human contributing factors.

Table 2. Examples of correlations between Design Failures and Human Factors in accidents from Cluster 3 (extracted from MATA-D).

Id.	Design Failure	Human Contributing Factors
1	Poor piping layout, pressure safety valve situation was not seen from the protected equipment site. An inspection of the safety valve in another location would have been required, in order to identify its removal. Poor layout, control room and quarters were located close to the compression module, and a fire/explosion would affect the response capacity and the evacuation of the crew. Fire walls were not blast resistant, and there were no redundancy for the deluge system manual activation.	Fire pumps were switched from automatic to the manual position aiming at the protection of divers, and when the explosion took the control room, it was impossible to activate them (no redundancy). Faulty diagnosis regarding the operational status of the pump (safety valve has been removed). Pump was started before the conclusion of maintenance services. The fire, explosion and collapse of the unit resulted in 167 fatalities.
2	Poor layout of the unit, hot exhaust pipes were located right above the riser area. Any hydrocarbon escape was likely to generate an explosion. Also, risers were not protected from heat or explosion between the waterline and emergency shutdown valves. Poor layout of the design change was also observed. Service was supposed to install a new accessory (pig trap) below shutdown valve. If it was designed to be installed above the shutdown valve, the service could have been carried out in a safer way.	Shutdown valve was left open (closing it could have limited the inventory and restricted the consequences of the explosion to the riser under service). Due to some difficulties to remove a blind flange, the riser content was not verified before cutting. After identifying a marginal condensate leakage, operator incorrectly predicted that it would stop and continued the cold-cutting service. A very significant condensate spray ignited and caused the remaining pipes to burst due to the intense heat. The accident resulted in 7 fatalities.
3	The conversion of a drilling unit into a production unit led to a poor layout, as hydrocarbon tanks were left in the legs of the unit, compromising the structural stability and buoyancy in case of an explosion.	The plan to drain an atmospheric storage tank was flawed, as the relief (vent) was sealed while the intake was not isolated. Sealing of the vent was performed before emptying the tank, causing the content to scape. Also, oily water was often (incorrectly) disposed in the drains tank. The explosion caused 11 fatalities.
4	Poor well design, no redundancy for hydrocarbon influx barrier in the well (well layout). Production casing was located in a way that additional risk of influx was created.	Plans to optimise operation by using a lock-down sleeve valve has brought additional difficulties in critical operations, including barrier tests. Pressure test was misinterpreted. Failed to observe well fluids balance (in/out) on mud tank, a strong indicative of a blowout. After the late detection of the hydrocarbon flow, it was directed to a mud-gas separator, a piece of equipment not designed to handle high flow rates. 11 people died as a consequence.
5	Poor platform layout: riser zone was vulnerable to the load zone (inadequate position and poor mechanical and fire protection); risers were too close as well as contiguous platforms, triggering a domino effect after the rupture. Position of the shutdown valve allowed 12km of inventory to fuel the fire.	Supply vessel captain decided to approach the platform from windward side, as the leeward crane was not operational. Approach to the platform was taken too far and the vessel collided with risers. 22 fatalities emerged from the fire and explosion.
6	Poor layout, reactors were grouped into identical sets of four, increasing the likelihood of human error. Interlock system was poorly designed, allowing easy bypass (It was controlled by procedures and training). No mechanism to prevent the opening of pressurised vessels.	Manager decided not to implement earlier recommendations to change the valve interlock bypass to reduce potential misuse. Operator misidentified the vessel he was cleaning, overrode the safety valve by connecting an air hose and opened the wrong vessel. 5 people died after the massive explosion and the destruction of the plant.
7	Contents of a tunnel to transfer water from a supply system was being discharged in a room with limited natural ventilation. Poor design of the ventilation system (discharge system was not open to atmosphere; wrong position/layout of vents)	Operator decided not to open washout valve periodically (as recommended) and let it partially opened all the times. The intention of his plan was to minimise the discoloration of a river every time the valve was fully opened. A void in

	limited the capacity to disperse gas, and allowed the creation of an explosive pocket. Concrete-lined tunnel was not designed to be watertight nor positively pressurised, thus ground water from the surrounding environment (containing natural gas) leaked in the tunnel.	the tunnel was created, allowing the influx of gas from the surrounding formation. The explosion killed 16 people.
8	Poor layout, a 500-gallon propane tank was located against the building external wall, allowing propane to go into the administrative building when a release took place, after an inadequate plug removal.	The operator removed too fast a plug from the tank, not allowing sufficient time to observe a small stream of propane through the telltale (a hole drilled through the threaded plug), which would have gradually exposed a valve leakage. 4 people died after the destruction of the building.
9	Poor design (material selection). Aboveground piping for a methanol system was from polyvinylchloride (PVC) instead of steel or iron. Storage tank contained an aluminium flame arrester, which was corroded by the methanol.	An operator started using a cutting torch on a roof above the methanol tank without checking the surrounding atmosphere. Vapours coming from the tank were ignited, and the flame arrestor failure let the tank explode, killing 2 workers.
10	Poor design (material selection). The usage of S30400 and S31600 alloys for stressed components, associated with the chloride and moisture rich atmosphere, led to a catastrophic chloride-induced stress corrosion cracking in chrome-nickel steel bars supporting a ceiling. Also, there was no structural redundancy for the support of the suspended ceiling.	During a routine inspection, inspectors wrongly attributed the observed damage to some construction error, and repaired by welding a bar from the same material, without further investigation. They ignored the possibility of stress corrosion. The ceiling collapse killed 12 people.
11	Poor design of a group of three independent sensors, which were prone to simultaneous icing. This led to the loss of airspeed indications in the cockpit of a commercial airplane. Facing multiple alarms and error messages and no specific unreliable speed detection prompt, the crew was unable to diagnose the problem by interpreting the computer output.	Pilot failed to identify the deviation of the flight path, the unreliable airspeed and the approach to stall. Then, failed to diagnose the stall situation, lacking actions that would have made recovery possible and performing inappropriate control inputs. Ultimately, pilot had built a wrong mental plan, trying to apply at high altitude a control strategy recommended for low attitudes.

Results largely suggest that most of the design inadequacies can be traced back to earlier stages of the design development, where a basic design correction – i.e. changing the facilities' layout or better specification of materials employed – would be viable if detected on time by a reviewing process.

5 DISCUSSION

The significance of design failures as a major accidents contributor and its connections with human errors have been highlighted by the events grouped in Cluster 3. The accidents from this cluster undoubtedly brought the deepest consequences to human life, represented by a fatality rate of 19.71 deaths per event, the most significant figures among all groupings by far. Cluster 3 also contained the largest figures for design failures (87.5%).

The scrutiny of the interfaces among design failures and other contributing factors can help establishing mechanisms to manage design from a hazard mitigation perspective.

A general checklist, presented in the bullet points below, can be derived from the findings of this work. The checklist is intended to guide designers and the people responsible for reviews in the search for problems, design shortcomings and improvement opportunities. Good examples are the correlations 1, 2 and 8 in Table 2, which inspired the first and the second bullet recommendations to designers, regarding layout (distances among modules and protection of the control room). The third and fourth bullet points derived from the correlation number 6, and so on.

Therefore, a reasonable start point would be to focus on the layout or general arrangement of the designed facility, taking into account the following lessons learned from Cluster 3 accidents:

- Accommodation, resting and leisure facilities, administrative offices and parking spaces, must be located within a safe distance from the process facilities and any hazardous materials;
- Control rooms must be protected from damage and located within a safe distance from the process plants. A scenario of control room loss must be included in safety analyses, and redundancy of emergency controls (e.g. fire control system, shutdown systems) must be designed;
- Reactors, vessels and equipment arrangement and dimensions should take into consideration a perception perspective, being visually distinctive to allow a human operator to differentiate them immediately, e.g. by the position, size or colour.
- Electrical, mechanic and hydraulic connectors should not be interchangeable among different systems or functions – any inadvertent connection must be avoided by design.
- The isolation indication of safety valves meant to protect equipment and systems

against overpressure must be directly observable from the protected equipment, and inadvertent operation must be prevented by mechanical barriers;

- Ignition sources (e.g. exhaustion, electrical equipment) must be located away from piping carrying significant amounts of hazardous materials, or in a position in which ignition is minimised in case of leakage;
- Strategies to limit the released inventory in case of piping leakage must be provided, such as the installation of automatic emergency shutdown valves (ESDVs). Surrounding equipment should withstand a release followed by a jet fire for the inventory depletion time, i.e. the time to consume the combustible between two safety valves;
- Mechanical protection should be provided where collisions and explosions are possible;
- Distance among adjacent equipment should be sufficient to avoid domino effects and escalation. Blast and fire protection should be considered;
- Safety barriers prone to common cause failures should be considered to be a single barrier. The same concept applies to sensors and alarms. If alarms and sensors are subjected to the same failure modes, e.g. same power supply, they cannot be considered redundant;
- Design should consider redundancy as fully independent safety barriers to protect systems or structures from critical scenarios;
- Where the creation of explosive atmospheres is likely, safety measures should be provided, such as the installation of deluge or inerting (CO_2 or N_2) systems; exhaustion/vents, if the flammable source is confined; usage of positively pressurised rooms, paths or tunnels and/or provide automatic shutoff for air inlets, if the flammable source is external;
- In case of an accident scenario, a safe evacuation path including anti-blast and fire walls must be provided. The escape route must contain indication if it is clear for use, by visual and audible alarms. Manual alarm switches to alert the remaining workers to evacuate the plant should be also provided;

In addition, the observed interfaces between design flaws and human behaviour indicated some improvement points, as listed below.

- To minimise the result of delayed or improper responses from operators (such as in examples 4 and 11), systems must be designed to interpret strong signals and respond promptly. When signals (e.g. significant changes in fluids in/out balance in a well or multiple alarms) can be translated in a clear action (automatic shut-in), the system must act autonomously;
- Situations involving multiple alarms are especially prone to automatization, as the variety of alarms and signals are likely to cause many adverse effects in human behaviour. Humans may tend to take into account only the information which confirms their assumptions (i.e. a confirmation bias), select a wrong objective to stabilise the system or use incorrect criteria to diagnose the situation. When an automatized action is not applicable, the system should be able to provide single and clear messages to help diagnosing the problem;

Lastly, problems related to material selection are likely to be minimised if the following recommendations are taken into consideration.

- The chemical and mechanical properties of materials should be compatible with the environment and the product carried (case of pipelines), to avoid corrosion, chemical attack, mechanical damage and other effects; Also, the design should take into consideration the environment temperature and the expected interaction among materials with different temperature gradients;
- Protection between different commercial alloys must be provided, to avoid galvanic corrosion. This includes the interfaces between equipment and its supports and fixation parts; Also, pipelines, elbows and connectors from distinct materials should be differentiated by dimension or thread type during design, to avoid parts interchangeability in an industrial plant;
- Special attention should be devoted to the possibility of stress corrosion cracking in stainless steels. The right nickel content of the alloy for the environment should be defined, and further control measures (e.g. stress relieve or cathodic protection) should be designed, when practical;
- Corrosion mechanisms emerging from the saturation of wet hydrocarbons with dissolved carbon dioxide and sour environments should also be carefully considered.

6 CONCLUSIONS

This work presented a straightforward framework, in a checklist format, for a design verification scheme, aiming at the avoidance of human errors through the design enhancement. The lessons arose from a selection of major accidents where design shortcomings interfaced with human errors to result in multiple fatalities.

The several examples described in Table 2, all extracted from Cluster 3, emphasised that improving the management of earlier stages of the design process could generate substantial opportunities to re-

duce human errors and the overall risk. Many of the design shortcomings revealed by this research were mostly associated with features usually defined when the system is in a premature phase, where many opportunities for design improvement are open.

Therefore, an effective design review method should be able to address broad issues such as layout, material selection and the design of alarms and emergency interfaces, especially in a phase of the facility's lifecycle where the cost of changes are significantly lower, i.e. from conception to detailed engineering and before construction.

The list is also intended to raise the designers' and design reviewers' general risk awareness, by delivering a logical and direct method to learn from major accidents and to apply the information in risk mitigation strategies, in a very practical way.

7 ACKNOWLEDGEMENTS

This study was partially funded by CAPES (Proc. nº 5959/13-6).

8 REFERENCES

Evans, A. 2011. Fatal train accidents on Europe's railways: 1980-2009, *Accident Analysis and Prevention 43*: 391-401.

Baysari, M., McIntosh, A. and Wilson, J. 2008. Understanding the human factors contribution to railway accidents and incidents in Australia, *Accident Analysis and Prevention 40*: 1750-1757.

Bellamy, L.J. et al., 2007. Storybuilder - A Tool for the Analysis of Accident Reports, *Reliability Engineering and System Safety. 92*: 735–744.

Bellamy, L.J. et al., 2013. Analysis of underlying causes of investigated loss of containment incidents in Dutch Seveso plants using the Storybuilder method. *Journal of Loss Prevention in the Process Industries 26*: 1039–1059.

Boy, G. A. 2013. *Orchestrating human-centered design*. London: Springer.

British Broadcasting Corporation (BBC) Europe. 2016. Germany train crash: Human error to blame, says prosecutor. *BBC World News, 16 February 2016*. http://www.bbc.com/news/world-europe-35585302.

Doell, C., Held, P., Moura, R., Kruse, R., and Beer, M. 2015. Analysis of a major-accident dataset by Association Rule Mining to minimise unsafe interfaces. *Proceedings of the International Probabilistic Workshop (IPW2015), Liverpool, UK, November 4-6, 2015*.

Hollnagel, E. 1998. *Cognitive Reliability and Error Analysis Method*. Oxford: Elsevier Science Ltd.

Kohonen, T. 2001. *Self-Organizing Maps*. 3rd ed. Berlin: Springer.

Kohonen, T. 2013. *Essentials of the self-organizing map*. Neural Networks 37: 52–65.

Kurosu, M. 2011. Human centered design. *Proceedings of the second international conference, HCD 2011, held as part of HCI International 2011, Orlando, USA, July 9-14, 2011*. Heidelberg: Springer.

Moura, R., Beer, M., Patelli, E., Lewis, J. & Knoll, F. 2015a. Human error analysis: Review of past accidents and implications for improving robustness of system design, *Proceedings of the 24th European Safety and Reliability Conference, 14–18 September 2014, Wroclaw*: 1037-1046. London: Taylor & Francis Group.

Moura, R., Beer, M., Patelli, E., Lewis, J. & Knoll, F. 2015b. Learning from Accidents: Analysis and Representation of Human Errors in Multi-attribute Events. *Proceedings of the 12th International Conference on Applications of Statistics and Probability in Civil Engineering, ICASP12 Vancouver, Canada, July 12–15, 2015*.

Moura, R., Beer, M., Doell, C., Kruse, R. 2015c. A Clustering Approach to a Major-Accident Data Set: Analysis of Key Interactions to Minimise Human Errors. *Proceedings of the 2015 IEEE Symposium Series on Computational Intelligence (SSCI2015), Cape Town, South Africa, December 8-10, 2015*.

Moura, R., Beer, M., Patelli, E., Lewis, J. & Knoll, F. 2016. Learning from major accidents to improve system design, *Safety Science 84*: 37-45.

Reason, J. 1997. *Managing the Risks of Organizational Accidents*. Farnham, Surrey: Ashgate Publishing Limited.

Swain, A.D. 1990. Human Reliability Analysis—Need, Status, Trends and Limitations. *Reliability Engineering and System Safety 29*: 301–313.

Ultsch, A. 1993. Self-organizing neural networks for visualization and classification. In Opitz, O., Lausen, B., Klar, R. (eds.). *Information and Classification*:307-313. Berlin: Springer.